NetVanta 2050/2054

Small Office and Home Office VPN Gateway and Firewall

Product Features

- Standards-based IPSec VPN tunneling with DES/3DES/AES encryption
- Internet Key Exchange (IKE) for user authentication
- Stateful inspection firewall for network security
- Five private tunnels and up to 15 users
- Built-in IP router supporting BGP, OSPF, and RIP
- Quality of Service (QoS) for delay sensitive traffic like VoIP
- Network Address Translation for IP address concealing
- Web-based and CLI remote management
- 10/100Base-T Ethernet interfaces for flexible connectivity
- Logging and alerts
- Industry-leading five-year North American warranty

The ADTRAN NetVanta® 2050 and 2054 are Small Office/Home Office VPN/Firewall gateways providing all the necessary components required to secure an integrated VPN solution. Used primarily for remote access, the NetVanta 2050 and 2054 are perfect for work-at-home telecommuters needing to have a secure connection back to corporate resources. Based on the ADTRAN Operating System (AOS), the NetVanta 2050 and 2054 provide key security and data protection features such as IPSec VPN tunneling, stateful inspection firewall, IP routing, Network Address Translation (NAT), and even a DHCP server. The 2050 and 2054 support the same features and perform the same functions, but the 2054 adds a built-in four-port 10/100Base-T Ethernet switcb.

Security

On a public infrastructure like the Internet, security is of the utmost importance. The NetVanta 2050 and 2054 employs a stateful inspection firewall that protects an organization's network from common Denial of Service (DoS) attacks including TCP synflooding, IP spoofing, ICMP redirect, ping-of-death, and IP reassembly problems.

For the telecommuter that needs a dedicated firewall without corporate VPN access, the NetVanta 2050 and 2054 offer a firewall only version. The firewall only versions offer the same basic features, without IPSec VPN tunneling, encryption and authorization.

VPN Tunneling

The NetVanta 2050 and the 2054 are IPSec-compliant devices that provide secure communications over potentially unsecure networks. As security gateways, both the NetVanta 2050 and 2054 supports up to five simultaneous VPN tunnels and up to 15 users on the LAN, while supporting encryption algorithms including DES, 3DES, and AES. In addition, these devices support IKE (Internet Key Exchange) and X.509 digital certificates for user authentication.

Management

NetVanta's web-based GUI or CLI can be used for secure local or remote configuration of any NetVanta 2050 and 2054. For a centralized, enterprise-wide management scheme, ADTRAN offers n-Command™, an intuitive, scalable software suite for managing larger NetVanta deployments and features robust productivity tools to effectively manage a distributed network. To administer user accounts, the NetVanta 2050 and 2054 utilizes XAUTH using RADIUS and RSA SecurID to manage administration account lists. These devices also offer built-in alert and logging mechanisms to warn administrators about activities that are going on in the network.

Quality of Service (QoS)

QoS is also supported for delay sensitive traffic like VoIP or video. To prioritize mission critical traffic and control network congestion, the NetVanta 2050/2054 uses Low Latency Queuing, Weighted Fair Queuing (WFQ), Class-based WFQ, and DiffServ marking to establish priority of IP packets routed over the network.

VoIP Ready

In combination with the QoS features, a specialized SIP Application Layer Gateway (ALG) allows SIP traffic to traverse NAT-enabled firewalls. For an enterprise network, this interoperability allows IP PBXs, pbones, and other SIP-based devices to set up, tear down, and pass voice and call control messages seamlessly through the integral NAT-enabled firewall.

Interoperability

The NetVanta 2050 and 2054 offers the highest level of integration with ADTRAN's complete line of IPSec VPN equipped NetVanta products: NetVanta Ethernet Switches, NetVanta Access Routers, and NetVanta VPN/Firewall appliances. Together the NetVanta Series offers the most robust set of feature to address a wide range of enterprise VPN needs.

Downloaded from www.Manualslib.com manuals search engine

Copyright © 2013. Acer Incorporated.
All Rights Reserved.

Acer Projector X1263/P1163/X1163/X113 Series User's Guide
Original Issue: 01/2013

Changes may be made periodically to the information in this publication without obligation to notify any person of such revisions or changes. Such changes will be incorporated in new editions of this manual or supplementary documents and publications. This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims the implied warranties of merchantability or fitness for a particular purpose.

Record the model number, serial number, purchase date and place of purchase information in the space provided below. The serial number and model number are recorded on the label affixed to your projector. All correspondence concerning your unit should include the serial number, model number and purchase information.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronically, mechanically, by photocopy, recording or otherwise, without the prior written permission of Acer Incorporated.

Acer Projector X1263/P1163/X1163/X113 Series

Model number: _____

Serial number: _____

Date of purchase: _____

Place of purchase: _____

Acer and the Acer logo are registered trademarks of Acer Incorporated. Other companies' product names or trademarks are used herein for identification purposes only and belong to their respective companies.

"HDMI™, the HDMI logo and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC."

Downloaded From projector-manual.com Acer Manuals

Downloaded from www.Manualslib.com manuals search engine